IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA v. ALEKSEI YURIEVICH BURKOV, Defendant.	Case No. 1:15-CR-245 Hon. T.S. Ellis, III

POSITION OF THE UNITED STATES ON SENTENCING

"There's no honor among thieves." That adage captures an age-old problem for criminals: they can achieve more lucrative crimes if they work together, and yet, the people who would be their partners-in-crime are often by their very nature untrustworthy. This problem is even more acute in the cybercrime world, both because the complex nature of the work often requires cooperation among criminals with different skills and resources, and because the anonymous nature of the internet makes trusting fellow criminals particularly fraught. A cybercriminal could commit exponentially more crime if there was a website where he or she could buy hacking tools, rent access to compromised computers, find associates to help with the leg work, and access a black market for the wholesale distribution of large amounts of hacked financial information. But even if such a website existed, how would you trust the people on the website not to rip you off? There is, after all, no honor among thieves.

Aleksei Burkov's website, Direct Connection, was an attempt to solve this dilemma. From 2009 to 2015, Direct Connection was the most exclusive criminal forum on the web, accepting only those who had developed a reputation for fair-dealing in the online criminal underworld. To even be put up for a vote, prospective Direct Connection members needed three existing members to "vouch" for them and to provide $5,000 in insurance in case the applicant reneged a deal formed while conducting business on the forum. Direct Connection was used to advertise illicit goods, such as personal identifying information and malicious software, as well as criminal services, such as money laundering and hacking. Burkov offered escrow services to facilitate criminal deals and appointed an "arbiter" who would resolve disputes between Direct Connection members. As a result of its organized and exclusive nature, Direct Connection's several hundred members were a veritable Who's Who of the world's most notorious cybercriminals.

In addition to Direct Connection, Burkov also ran a website called "Card Planet," which sold stolen credit and debit card numbers on a massive scale, victimizing hundreds of thousands and resulting in over **$20 million in fraud**. The presentence report correctly calculated the Guidelines at the statutory maximum of 180 months. The government respectfully submits that a sentence of **180 months** is necessary to reflect Burkov's immense contribution to organized cybercrime and to deter this novel and rapidly-growing type of crime.

I. Offenses of Conviction

Burkov, a Russian national who resided in St. Petersburg, Russia, was arrested at Ben-Gurion airport near Tel Aviv, Israel, on December 13, 2015, based on a provisional arrest request from the United States. Over the next four years, the Russian government went to great lengths to thwart Burkov's extradition to the United States, including by filing its own extradition request. An Israeli district court approved Burkov's extradition in 2017. He was extradited to the United States on Nov. 11, 2019, after appeals to the Israeli Supreme Court and the Israeli High Court of Justice were denied.[1]

On January 24, 2020, Burkov pled guilty to Conspiracy to Commit Identity Theft, Access Device and Wire Fraud, Computer Intrusions, and Money Laundering, in violation on 18 U.S.C. § 371, and a substantive count of Access Device Fraud, in violation of 18 U.S.C. § 1029(a)(3). The conspiracy count arose from his operation of Direct Connection, whereas the access device fraud count arose from his operation of Card Planet. In connection with his guilty plea, Burkov admitted to the facts set forth immediately below.

[1] The defendant was detained in Israel from December 13, 2015, through November 10, 2019, pursuant to a provisional arrest request from the United States for charges connected with this case, and not based on any crime under Israeli law. Accordingly, the Bureau of Prisons should count that time towards the sentence the Court imposes in this case and will do so unless the Court orders to the contrary. *See* 18 U.S.C. § 3585(b)(1).

A. Direct Connection

Burkov and a partner founded Direct Connection in 2009. PSR ¶ 16. Burkov organized Direct Connection into numerous sections where members could post comments on different topics. PSR ¶ 19. These sections, known as "forums," were labeled as follows:

- News
- Stuff Carding-Drops for Stuff, Online Shopping
- Buying and Selling Cards, Visa, MasterCard, and Amex, Looking up SSN/DOB and other card holder information.
- Real Carding, Documents, Real Plastic, Equipment, Dumps (cashing/sales)
- Banking, Drops, account cashing, bank transfers
- Information Security, programing, intrusion, databases, botnets, Trojans, scripts and exploits.

PSR ¶ 19.[2] As indicated by their titles, these forums covered such topics as credit card fraud, money laundering, malware, and hacking. *Id.* In particular, "carding" refers to buying and selling stolen payment card information; "looking up by SSN/DOB and other card holder information," refers to services that allow cybercriminals to search for personal identifying information of particular victims; "dumps" refers to stolen payment card information; "botnets" refers to networks of compromised computers; "drops" and "bank

[2] All quotations in this memorandum of statements made on Direct Connection were translated from Russian by government translators.

transfers" refer to money laundering services; and "trojans" and "exploits" are hacking tools.

Direct Connection members could create "threads" on each forum to discuss a designated topic by posting comments to that thread. *Id.* Examples of some of the posts on Direct Connection include members soliciting or advertising stolen data, members selling hacking tools, and members offering money laundering services. *Id.* For example:

- On May 22, 2015, under the forum, "Banking. Drops. Accounts" and the thread "Banks. Accounts. Cash-out of bank transactions. How to work with drops. Merchants," a Direct Connection member posted: "Looking for continuous deposits on US prepaids. Quick cash-out on a POS with a daily limit."

- On August 8, 2011, under the forum "Cards to sell and to buy," a Direct Connection member posted, "We're selling USCC [United States Credit Cards] with a known available balance. 100% validity. It's possible to pick by the state. Prices: $5 for a CC + $0.5 for every 1K," and provided his email address.

- On May 27, 2010, under the Forum "Real plastic. Equipment, dumps (cash-out, sale). Documents and scans," a Direct Connection member posted: "Looking for people to withdraw the entire balance from US D+P. Balances start from 50K. Please PM me contacts and your interest rate." "US D+P" refers to stolen U.S. debit cards ("dumps") along with the corresponding pin number. The purpose of this post was to solicit assistance with stealing money from compromised U.S. debit card accounts.

- On June 20, 2010, under the forum "Banks Accounts Cash-out of bank transactions. How to work with drops. Merchants," a Direct Connection member provided advice on how to launder money from U.S. banks, posting: "You can open an account online almost in every bank in the US, that's correct. The

problem is that banks check addresses in public records and can ask you to come to their branch to confirm."

- On November 3, 2015, under the forum, "Spam Downloads and traffic. Hosting, domains and servers," and the thread, "Sales and purchase of downloads and traffic," a Direct Connection member posted: "I need US and EU loads for a quiet and compatible software. I'm ready to align with almost anything except lockers, fake AV and other aggressive software. If you load a formgrabber, clicker, socks bot, or suchlike, please PM and we can agree on terms." This post offered web-hosting services to be used for computer hacking schemes.

- On November 20, 2015, a Direct Connection member posted an advertisement indicating he wished to sell a database containing the names and dates of birth of over 191 million Americans. This database contains the personal information of American citizens, including some residing in the Eastern District of Virginia.

PSR ¶ 19.

"PMs," as used above, refers to the "Private Message" feature of Direct Connection that enabled members to speak directly with one another over the Direct Connection platform. PSR ¶ 20. As intended by Burkov, members who wished to engage in criminal schemes together would often respond to a public post with a private message. *Id.* Private messages often led to members exchanging contact information and continuing to work together off the platform. *Id.* For instance, Direct Connection members sent each other the following "PMs" over Direct Connection:

- On November 21, 2012, a Direct Connection member private messaged another member asking, "Regarding logs, I have some from 2011 and 2012, I can try and

find about 200 Gb. How much do you pay and how much do you want to take? What else do I need for the account except the login and password?" This message concerned selling stolen login credentials.

- On December 15, 2012, a Direct Connection member private messaged another member: "I'm writing regarding drops in the US. How can I contact you?" This message concerned laundering stolen money in the United States.

- On July 13, 2013, a Direct Connection member private messaged another member, asking "What kinds of goods are available and what is the approximate volume? I'm not a professional buyer, but I'm interested in buying in the US." This message concerned the sale of stolen U.S. payment card data.

- On February 17, 2014, a Direct Connection member private messaged another: "I have a lot of logs and I'm interested in work on an ongoing basis. Write if you need anything specific." The message concerned working together to extract login credentials to financial accounts from data stolen via computer hacking.

- On May 7, 2010, a Direct Connection member private messaged another member in response to a post about withdrawing money from compromised U.S. debit card accounts, stating "I have an interesting offer for your question. If you have a good volume of D+P with a decent balance, I can deposit a good volume … Let's connect in Jabber, I'll tell you all the details! Different schemes!"

- On October 10, 2011, a Direct Connection member private messaged another member, providing information about a bank account at a major bank in Hyattsville, Maryland, that included the account number and wire routing number. This message concerned making unlawful transactions from that account.

- On November 14, 2011, a Direct Connection member private messaged another member: "I'm selling the

> license for a 100% private software (bank trojan). Expensive," and provided an email address. This message concerned the sale of malware to be used in computer intrusions.

PSR ¶ 20.

Burkov designated a number of co-conspirators with leadership positions on Direct Connection. This included approximately a dozen "Moderators" (whose job it was to moderate the discussions on the particular forums to which they were assigned), a person in charge of escrow services to facilitate criminal deals among Direct Connection members, and an "Arbiter" who adjudicated disputes between Direct Connection members. PSR ¶ 21.

The "Arbiter" would adjudicate "suits" that Direct Connection members would file against each other in the event that the criminal agreements made on Direct Connection gave rise to disputes. PSR ¶ 23. Members who did not abide by the decisions of the Arbiter with regards to these "suits" could be expelled from Direct Connection. The following is an example of a "suit" filed by one Direct Connection member against another, accusing the other member of failing to provide agreed-upon "logs," which refers to information stolen via computer hacking, potentially containing login credentials or financial information. Following the formality required by Direct Connection, the Direct Connection member posted the following to the forum:

> I, [redacted], am aware of the Forum's terms and conditions, am responsible for the accuracy of given facts and speculations, and am aware that as a result of this suit my opponent and I can lose our membership on the Forum. **Plaintiff:** [redacted]. **Defendant:** [redacted] **Case:** purchased accounts from logs, ignored in Jabber. **Cost:** 560 WMZ.

> **Description:** On March 14, 2014 I agreed to buy accounts from logs; this person answered that he would transfer the material the next day because at that moment he wasn't at his working computer. I agreed and transferred WMZ the same day. The next day I did not receive any accounts, nor did I receive them the day after. I was ignored; he answered me once in 3 days that he is busy etc. I was and am asking the defendant to send the money back as those logs are not important anymore, and we had agreed the time in the first place. I will send logs and contacts upon request.

PSR ¶ 23.

Direct Connection members would also post advice to assist each other in avoiding arrest. PSR ¶ 24. For instance, on April 11, 2014, a Direct Connection member posted a thread under the forum "News" regarding an article entitled, "Russian Ministry of Foreign Affairs: The growing threat of Russian citizens being detained on the USA demand." In the same thread, the Direct Connection member posted the following: "Here's a list of countries that practice extradition, if anyone's interested…."

Direct Connection's membership included some of the world's most elite cybercriminals, including but not limited to the following:

- Direct Connection member "Carlos," also known as "aqua," was one of the early members of Direct Connection and moderated the banking sub-forum for many years. Carlos used Direct Connection to advertise malware designed to steal banking information from victim computers. Carlos, whose real name is Maksim Yakubets, has been indicted in the Western District of Pennsylvania and the District of Nebraska for crimes arising from his use and distribution of malware. The State Department has offered a $5 million reward for information leading to his arrest or conviction.

- Direct Connection member "Harderman," joined Direct Connection in 2010 and used the forum to promote his malware products, including ZeuS banking trojan version 2.0 and later the SpyEye banking trojan. In 2016, "Harderman," whose real name is Aleksandr Andreevich Panin, was sentenced to 9.5 years in prison by the U.S. District Court for the Northern District of Georgia. Burkov personally vouched for Harderman's admission to Direct Connection, stating in 2010: "His software is worthy of respect, in my opinion it has already surpassed the long famous Ze[uS] :-) I've known him about a year, about as long as I've used his product. I am as happy as a clam about our cooperation, he always helped, he never lets a question go unanswered, in general he has provided support above and beyond. I confirm fin. responsibility $2,000."

- Direct Connection member "WebHost" offered a variety of criminal services to the Direct Connection members in a long-running Direct Connection thread titled "Hosting/Servers/Domains/VPS high-end quality." WebHost's real name is Mykhaylo Rytikov of Ukraine. Rytikov has been indicted in three federal districts in the United States, including the Eastern District of Virginia. The charges against Rytikov arise from, among other crimes, providing "bullet-proof hosting," *i.e.*, servers designed to be outside of the reach of law enforcement and used in criminal schemes.

- Direct Connection member "Centurion" was the moderator of the subforum for security and anonymity. This was one of several forums on which this person both occupied a position of authority and used that position to facilitate trafficking in stolen financial data. Centurion, whose real name is Sergey Vovnenko, was arrested in June 2014 and extradited to the United States. In 2017, Vovnenko was sentenced to 41 months in prison by the U.S. District Court for the District of New Jersey for operating a botnet, stealing login and payment card data, and related crimes.

PSR ¶ 22.

Burkov personally used Direct Connection to advertise his own criminal services, including Card Planet. PSR ¶ 25.

B. Card Planet

From October 23, 2011, through at least August 2013, Burkov ran a website called "Card Planet," which offered for sale over 150,000 stolen credit and debit card numbers. PSR ¶ 9. The stolen credit and debit card numbers offered for sale on Card Planet were primarily issued by U.S. financial institutions to persons in the United States. PSR ¶ 13. As intended by Burkov, customers who purchased stolen payment card data on Card Planet used the data to make fraudulent purchases using the credit lines and bank accounts of their victims. PSR ¶ 14. The known fraudulent transactions committed using stolen payment card data offered for sale on Card Planet exceeds $20 million. PSR ¶ 15.

II. Guidelines Calculations

The Presentence Report properly calculated the offense level as follows:

Guideline	Offense Level
Base Offense Level (§ 2B1.1(a)(2))	6
Loss amount between $65 Million but less than $150 Million (§ 2B1.1(b)(1)(K))	+24
Offense involved 10 or more victims (§ 2B1.1(b)(2))	+2
Offense involved receiving stolen property and the defendant was in the business of receiving and selling stolen property (§ 2B1.1(b)(4))	+2
Substantial part of offense committed abroad (§ 2B1.1.(b)(10))	+2

Offense involved trafficking in unauthorized access devices (§ 2B1.1(b)(11))	+2
Leadership role (§ 3B1.1(a))	+4
Acceptance of responsibility (Section 3E1.1)[3]	-3

PSR ¶¶ 38-50. This yields an offense level of 39. PSR ¶ 51. Given the defendant's Category I criminal history, this offense level would normally result in a Guidelines Range of 262-327 months. However, the statutory maximum sentences for the defendant's convictions under 18 U.S.C. §§ 1029(a)(3) and 371 are ten and five years, respectively. PSR ¶ 74. Accordingly, the defendant's guidelines range is capped at the combined statutory maximum of fifteen years' imprisonment. *Id.*

III. Sentencing Recommendation

As the Court is well aware, the Sentencing Guidelines are advisory, and just one factor that must be considered along with the other factors set forth in 18 U.S.C. § 3553(a).[4] Here, however, a Guidelines sentence is also supported by the other

[3] The Government hereby moves, under U.S.S.G. § 3E1.1(b), for a third level to be reduced from the defendant's offense level, based on the defendant's timely acceptance of responsibility.

[4] The § 3553(a) factors include: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed training, medical care, or other treatment; the kinds of sentences available; the kinds of sentence and the sentencing range established for the type of offense committed; any pertinent policy statement; the need to avoid unwarranted sentence disparities among defendants with similar records who have

§ 3553(a) factors, particularly the need for a sentence that reflects the seriousness of the defendant's immense contribution to organized cybercrime and adequately deters others from perpetrating similar crimes.

A. The Sentence Should Reflect the Defendant's Outsized Role in Global Organized Cybercrime.

The fifteen-year guidelines range in this case is largely driven by the loss amount of $75 million, which resulted in a 24-level enhancement under § 2B1.1(b)(1)(K). PSR ¶ 39. This loss amount was calculated by taking the 150,000 stolen credit and debit card numbers offered for sale on Card Planet and multiplying by $500 per access device as required by U.S.S.G. § 2B1.1, app. Note 3(f). Fraud defendants often challenge the $500/access device rule as overstating the financial harm. In this case, however, the government was able to confirm over $20 million in actual fraud committed using stolen credit and debit cards that were sold on Card Planet. PSR ¶ 15. So even if the standard were actual provable loss (which it is not), this would only reduce the offense level by 4 and, because of the statutory cap, would not reduce the fifteen year guidelines range at all. In short, the fifteen-year guidelines range does not overstate the immense actual financial harm in this case.

Moreover, the $75 million loss figure is based entirely on the stolen credit and debit card numbers sold on Card Planet and does not even consider the substantial harm caused by Direct Connection. As noted above, Direct Connection served a key role in bringing together, organizing, and building trust amongst hundreds of the

---

been found guilty of similar conduct; and the need to provide restitution to any victims of the offense.

world's most elite cybercriminals. By working together, these notorious actors were no doubt able to commit exponentially more crimes and more sophisticated crimes than any could have alone. *See* Ben Collier *et al.*, *Cybercrime Is (Often) Boring: Maintaining the Infrastructure of Cybercrime Economies*, at 1 (Cambridge Cybercrime Centre, 2020) ("It is generally accepted that the widespread availability of specialist services has helped drive the growth of cybercrime.") (hereinafter "Collier, *Cybercrime Economies*"), available at https://www.cl.cam.ac.uk/~bjc63/Crime_is_boring.pdf.

Tackling global cybercrime means punishing the leaders who have allowed cybercrime to become organized and hyper-specialized. In recent years, judges in this District have considered, at sentencing, the widespread harm that leaders and organizers of cybercrime inflict. *See, e.g.*, *United States v. Bondars et al.*, 1:16-cr-228 (E.D. Va.), Dkt. 233, at 23–26 (sentencing transcript containing Court's observation that defendant who created and operated a tool "facilitating, aiding and abetting enormous numbers of hackers" needed to be deterred and that seriousness of crimes warranted 168-month sentence). Here, Burkov made significant contributions to the organization of cybercrime by helping to overcome the "skill, trust, and funding barriers which inhibit the development of truly mass-scale cybercrime economies" and helping buyers "find sellers in scam-ridden underground communities." Collier, *Cybercrime Economies*, at 5. His sentence should reflect his central role in the global cybercrime ecosystem.

B. The Sentence Should Be Sufficient to Deter Others from Committing Similar Crimes.

By the defendant's own admission, cybercrime has been his main source of income throughout his life. PSR ¶¶ 71-72. Indeed, Card Planet alone took in at least $1,005,977.01 in revenue. PSR ¶ 6(f). It is no doubt the proceeds of cybercrime that funded the defendant's vacations to locations such as Thailand and Israel, among others. The defendant's lifestyle is relevant because it demonstrates a larger problem: cybercriminals like the defendant are often able to earn a steady income through internet-related crimes committed from the comfort of their living rooms. Like the defendant, these criminals often operate under aliases and do so undetected by law enforcement for years. All too many people are willing to commit crimes like the defendant's for a chance to live the comfortable lifestyle he enjoyed.

Unfortunately, high rewards and relatively low risk of detection are basic features of cybercrime that are not going to change anytime soon. As the Honorable J. Harvie Wilkinson, III recently observed in *United States v. Carver*, 916 F.3d 398 (4th Cir. 2019), an access device prosecution:

> Financial fraud is a modern scourge. It preys especially upon the unsophisticated and vulnerable. As the district court noted, crimes like those in this case harm victims 'in almost irreparable ways by causing them loss of work, mental anguish, monetary loss, and loss of peace of mind.' J.A. 152. It raises costs for businesses, which must invest in security measures. These crimes require time and expertise to investigate and can be difficult to unravel and prove.

Id. at 404.

The only way to affect the cost-benefit analysis of these crimes is to impose meaningful sentences on those who are caught Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor the government's response to cybercrime and plan accordingly, as the members of Direct Connection did for years. Achieving general deterrence in this area therefore appears particularly promising. *See United States v. Hayes*, 762 F.3d 1300, 1308 (11th Cir. 2012) ("[G]eneral deterrence is an important factor in white-collar cases, where the motivation is greed."); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (Because "economic and fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence" (internal quotations and citation omitted)); *see also* U.S.S.G. Ch. 1, Pt. A(4)(d) (explaining that the Sentencing Commission crafted serious economic crimes Guidelines in order to remedy the pre-Guidelines sentencing "problem" of courts imposing probation on an "inappropriately high percentage" of white-collar offenders).

IV. Conclusion

The government respectfully recommends a sentence of 180 months' imprisonment, as well as forfeiture and restitution orders in agreed-upon amounts.

G. Zachary Terwilliger
United States Attorney

By: /s/
Kellen S. Dwyer
Alexander P. Berrang
Assistant United States Attorneys
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700
kellen.dwyer@usdoj.gov

Laura Fong
Senior Trial Attorney
Computer Crime & Intellectual Property Section
Department of Justice
laura.fong@usdoj.gov

June 19, 2020

Certificate of Service

I hereby certify that on June 19, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to counsel of record for the defense.

I also certify that on or about the same date, I will send a true and correct copy of the foregoing by e-mail to the following:

William Byerley
United States Probation Officer
william_byerley@vaep.uscourts.gov

By: /s/
Kellen S. Dwyer
Assistant U.S. Attorney